УДК 681.3

ТЕХНИЧЕСКИЕ СРЕДСТВА ПРЕДНАМЕРЕННОГО НАРУШЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ СОЦИАЛЬНОЙ ИНФРАСТРУКТУРЫ

© 2021 Д. Е. Орлова

Воронежский институт ФСИН России (Воронеж, Россия)

Дается краткий обзор современных технических средств, которые могут использоваться злоумышленниками и преступными элементами для преднамеренного нарушения безопасности критически важных объектов социальной инфраструктуры. Приведенные данные могут найти применение в органах, обеспечивающих безопасность этих объектов, а так же при моделировании и оптимизации процессов обеспечения комплексной безопасности.

Ключевые слова: безопасность, критически важный объект, техническое средство.

Введение. Одно их основных направлений развития теории и практики управления в социальных и экономических системах связано с обеспечением безопасности критически важных объектов социальной инфраструктуры – КВОСИ [1-3]. Типичными примерами таких объектов являются правительственные здания и сооружения, учреждения внутренних дел и уголовно-исполнительной системы, отраслевые, территориальные и общегосударственные коммуникационные и логистические сети, крупные торговые и спортивные комплексы. В настоящее время эта проблема приобретает особую значимость, что обусловлено, с одной стороны, происходящим переоснащением КВОСИ электронными и компьютерными средствами обеспечения безопасности, а с ругой стороны, адекватным развитием средств преодоления барьеров безопасности. Уже сегодня злоумышленники и преступные элементы располагают достаточным арсеналом таких средств. Более того наблюдается постоянное совершенствование приемов, методов и технических средств деструктивных воздействий на компоненты системы обеспечения безопасности КВОСИ.

Цель статьи – дать краткий обзор современных технических средств, которые могут использоваться для преднамеренного нарушения безопасности КВОСИ.

Общая классификация технических средств нарушения безопасности, составленная на основе обобщения данных открытых источников [4-12], приведена на рисунке.

К средствам ведения криминальной разведки относят: мини-радиозакладки; стетоскопы; фиброскопы; приборы для съема информации с телефонных линий связи; аппаратуру для съема информации с окон с помощью лазерных излучателей; специальные фото-кино устройства; миниатюрные GPS-маячки; приборы ночного видения.

Мини-радиозакладки («жучки») – это подслушивающие устройства (стационарные и мобильные), которые злоумышленники могут тайно устанавливать в помещения, где предполагается вести подслушивание. Стационарные «жучки» питаются от электрической сети и обычно размещаются в настольных лампах, телевизорах, розетках, люстрах, удлинителях, тройниках, бытовой электротехнике. В качестве канала передачи информации используется силовая сеть 220В. Такие «жучки» работают неограниченное время, а информация от них принимается специальными приемниками, которые подключаются к силовой сети по длине проводки до силового трансформатора, обслуживающего здание. Мобильные «жучки» закладываются при тайном или легальном посещении целевого помещения (посетителями, уборщицами, подсобниками, всевозможными контрольными либо ремонтными службами) в самые укромные места (за книги, среди бижутерии, в обивке мебели) и нередко маскируются под шариковые ручки, коробки от спичек, безделушки и прочие непритязательные вещицы. Они могут преподноситься как сувениры (микрокалькуляторы, зажигалки), подменять наличные образцы канцелярских принадлежностей, а иной раз забрасываться в приоткрытую форточку. Существуют «жучки» – акустические закладки, работающие в инфракрасном диа-

Орлова Дарья Евгеньевна – Воронежский институт ФСИН России, адъюнкт, dasha_scorobogat@mail.ru.

пазоне. Но слышать их можно только в зоне прямой видимости. Поэтому они устанавливаются обычно у окон или вентиляционных отверстий. Даже хорошим сканером трудно обнаружить такие акустические закладки.

Рисунок. Технические средства преднамеренного нарушения безопасности критически важных объектов социальной инфраструктуры

Стетоскопы. Под стетоскопом понимают устройство (прибор) для подслушивания ведущихся за какой-либо преградой (стена, окно и пр.) разговоров или улавливания определенных звуков (например, шумов работы механизма сейфового замка или вибрации работающей за стеной шифровальной машины и щелчков ее дисков). Стетоскопы применяют в тех случаях, когда нельзя установить устройство съема информации непосредственно на месте. Принцип работы этого устройства таков: плотно прижатый к прослушиваемой поверхности (стене, перегородке или двери) чувствительный микрофон передает ее колебания на усилитель, от которого сигнал идет на головные телефоны. В отдельных случаях в помещении, из которого ведется подслушивание, устанавливается ретранслятор, который через эфир параллельно транслирует на закрытой частоте сигнал на постоянный пост подслушивания (где производится запись на профессиональную стационарную аппаратуру). При длительном подслушивании с помощью этого стетоскопа можно микрофон приклеить к стене клейкой лентой, что избавит агента от постоянного удерживания руки с микрофоном на весу. Такой прибор дает возможность осуществлять прослушивание разговоров через стену толщиной до 1 м и более (в зависимости от материала стены).

Фиброскопы. Это приборы подсматривания, в которых используются принципы волоконной оптики. Одним из доступных фиброскопов является модель *Pentax FNL-10rbs*. Его световод состоит из 7500 волокон. Изображение выводится на окуляр, а при выдвинутой антенне – передает видеосигнал на приемное устройство. Фиброскоп позволяет «проникать взором» сквозь щель (отверстие) размером 5 мм в стене, потолке, замочной скважине, вентиляционное отверстие на глубину до 120 см при секторе обзора в 60°. Аппарат позволяет увеличивать изображение в 10 раз и имеет микрофон, позволяющий вести параллельное подслушивание. Допустимый радиус изгиба световода – 3 см. В рукояти пистолетного типа расположены батарейка и лампочка, что позволяет освещать рассматриваемый объект через световод. Существуют модели фиброскопов, позволяющие вести съемку в инфракрасном свете и под водой.

Приборы для съема информации с телефонных линий связи встраиваются в телефонные аппараты и передают информацию через телефонную линию при положенной на рычаг трубке. Для каждой стра-

ны разрабатываются свои модели, соответствующие стандартным аппаратам известных фирм, которые там наиболее распространены. Например, для Германии это немецкая «*Alpha*»; для Юго-Восточной Азии – северокорейская «*Automatic*», для Голландии – «*Ericson*». Аппараты «Спектр» и «Телком» – для России. Еще одним подслушивающим устройством может быть так называемый отвод. Простейший способ установки отвода – это подсоединение второго аппарата к уже существующему телефону. Однако при снятии трубки слышится щелчок. Избежать этого злоумышленники могут путем установки специального «обходного аппарата», который позволяет слушать телефонный разговор, не поднимая трубку. Это устройство устанавливается путем подсоединения его к пазу позади любого стандартного настольного аппарата, причем разговор слушают при помощи наушников. Поднимать рычаг дополнительного аппарата не требуется. Также возможно прослушивание так называемой «ВЧ наводкой», когда к одному телефонному проводу подключается высокочастотный генератор, а к другому – амплитудный детектор с усилителем. При помощи такой системы помещение также может прослушиваться через телефон, на котором лежит трубка. Через телефонный аппарат можно слушать разговоры в комнате, используя и «звонковый эффект». Звонок телефона работает как микрофон, он передает в линию сигнал достаточной силы, такой, чтобы его можно было принять, усилить и записать.

Наименее защищены от подслушивания разговоры по сотовым телефонам, нужно просто подобрать его частоту и настроить на нее приемник. В отличие от телефонных жучков, встраиваемых в аппарат, при способе так называемой наружной активации к контролируемому телефону здесь даже не прикасаются. Информация снимается с сотового телефона при выключенном аппарате путем внешней активации высокочастотными колебаниями его микрофона, а порой и через перехват микротоков появляющихся в электромагнитном звонке при легчайших сотрясениях его подвижных частей за счет таг называемого «микрофонного эффекта». Стандартный микрофон, находящийся даже в нерабочем положении, испускает слабые импульсы, которые могут быть выделены и преобразованы в звуковые колебания. При этом каждый сотовый телефон становится «жучком», с которого злоумышленники могут снимать нужную им информацию.

Аппаратура для съема информации с окон с помощью лазерных излучателей. Лазерный микрофон, считывающий вибрацию оконных стекол и преобразовывающий ее в речь, позволяет слушать разговор в помещении через окно на расстоянии до 300 метров от него. Для работы большинства таких систем нужно предварительно нанести на стекло маленькое пятнышко специальной краски, которая отражает лазерный луч обратно на принимающее его устройство. Существует система и без использования пятна краски, но она сложнее в работе. Инфракрасный луч гелий-неонового лазера позволяет снимать звук с оконных стекол посредством измерения вибраций стекла тонким невидимым лучом. Направленный передатчиком, находящимся за сотни метров от стекла, луч под определенным углом отражается от него и принимается на специальное устройство с фильтрами паразитных шумов, расшифровывается и переправляется на магнитный носитель или на распечатку. Такие устройства малогабаритны и экономичны, тем более что в качестве приемника нередко используются фотообъективы с большим фокусным расстоянием, позволяющим вести перехват сигналов с дальних расстояний. Принцип действия лазерного устройства заключается в посылке зондирующего луча в направлении источника звука и приеме этого луча после его отражения от каких-либо предметов. Этими предметами, вибрирующими под действием окружающих звуков как своеобразные мембраны, могут быть стекла окон, шкафов, зеркала, посуда и т. п. Своими колебаниями они модулируют лазерный луч, приняв который через приемник можно достаточно просто восстановить звуки речи.

Специальные фото-кино устройства. В настоящее время эти устройства стали едва ли ни самыми распространенными при ведении криминальной разведки. Фото и киносъемка осуществляются с помощью современной аппаратуры и при дневном освещении, и ночью, на близком расстоянии и на удалении, в видимом свете и в инфракрасном диапазоне. Современные фото- и киноаппараты обладают чрезвычайно большими возможностями. Так, известны камеры размером со спичечный коробок, однако четко снимающие печатный текст на расстоянии до 100 м. А миниатюрные фотокамеры в наручных часах позволяют

делать фотографии с расстояния от 0,1 метра без наводки на резкость, установки выдержки и диафрагмы и передавать их по мобильным сетям.

К другому типу устройств, позволяющему считывать с листа и запоминать его содержание, относится сканеры. Эти приборы, размером чуть больше ладони, снабжены микропроцессором, запоминающим информацию. Сканер помещают вплотную к поверхности снимаемого документа и проводят им по странице. Если размеры листа превосходят ширину считывающего окна сканера, то съемка осуществляется в несколько проходов (проводок). Процессор запоминает отдельные части документа и самостоятельно соединяет их в единое целое. Для последующего прочтения информации сканер подключается к компьютеру, изображение выводится на монитор и может при необходимости распечатываться на принтере или анализироваться специальными программами.

Миниатюрные GPS-маячки. Эти приборы, размером меньше четверти спичечного коробка, помогают злоумышленникам обнаружить местоположение конкретного человека, а также установить траекторию движения специального транспорта. GPS-маячки могут подкладывать в карман или сумку отслеживаемого человека или прикреплять к контролируемому транспортному средству. Прибор может работать в режиме ожидания более одной недели от встроенного аккумулятора. Для того чтобы запросить координаты местонахождения GPS-маячка, необходимо сделать звонок на номер сим карты, которая будет установлена в маячке. Через несколько секунд придет ответ, с точными координатами. Кроме того, на маячок можно позвонить и услышать всё, что происходит вокруг в радиусе до трех метров.

Приборы ночного видения (ПНВ) – класс оптико-электронных приборов, обеспечивающих изображение местности (объекта, цели и т.п.) в условиях недостаточной освещённости. Приборы данного вида нашли широкое применение в деятельности преступных организаций для ведения скрытного наблюдения в тёмное время суток и в тёмных помещениях, вождения машин без использования демаскирующего света фар Современные ПНВ выпускаются в нескольких форм-факторах. Наиболее простым является ночной монокуляр – удерживаемая в руке оператора зрительная труба, обычно невысокой кратности. Бинокли ночного видения имеют два электронно-оптических преобразователя (ЭОП) и выводят увеличенное стереоскопическое изображение. Очки ночного видения – закрепляются на голове, имеют широкое поле зрения и не увеличивают изображение. Очки могут иметь два ЭОП либо быть псевдо бинокулярными, когда изображение с одного ЭОП поступает на оба окуляра. Монокуляр кратности 1×, закреплённый на оголовье, может использоваться как альтернатива очкам. Прицелы ночного видения закрепляются на оружии, как правило, увеличивают изображение и имеют прицельную сетку. Существуют также приставки ночного видения к дневным оптическим прицелам.

Средства криминального поджога. Анализ практики преступлений, связанных с поджогами, показывает, что чаще всего в качестве средств совершения поджогов используют: 1) средства, находившиеся на месте поджога; 2) заранее припасенные средства; 3) технические приспособления немедленного действия; 4) приспособления, рассчитанные на последующее загорание; 5) создание условий самовозгорания [21].

К *средствам, находившимся на месте поджога*, относятся все легковоспламеняющиеся материалы, которые могут попасть в поле зрения злоумышленника в месте, где он намеревается совершить поджог. Ими могут быть бумага, сено, солома, березовая кора, сосновая лучина, вата, промасленная ветошь и тряпки, а порой и такие легковоспламеняющиеся жидкости, как бензин, керосин и т. д.

Заранее припасенные средства. Готовясь совершить поджог того или иного объекта, злоумышленники заранее приобретают или подготавливают различные горючие вещества. Чаще всего ими бывают легковоспламеняющиеся и горючие жидкости, являющиеся продуктами нефти, растворителями, спиртами, эфирами, растительными маслами, олифой и т. п.

Технические приспособления немедленного действия используются, когда преступник не в состоянии подойти к объекту, намеченному им для поджога, в удобное для него время или проникнуть туда. Такие приспособления состоят обычно из фитиля различной длины и серы, пороха или взрывчатки.

К техническим приспособлениям, рассчитанным на последующее загорание,

относятся: электроприборы, химические реакции, часовые механизмы, горящие запалы и др. С целью поджога злоумышленники часто прибегают к использованию электробытовых приборов, включенных в сеть и окруженных легковоспламеняющимися материалами. Иногда на включенную электрическую лампочку набрасывают легкую ткань или бумагу. Бывают случаи, когда поджигатели специально оголяют электропровода с целью вызвать короткое замыкание. В практике имеют место факты поджогов при помощи испорченного электрического патрона. В ряде случаев злоумышленники совершают поджоги при помощи химических веществ. Известны случаи поджогов при помощи желтого фосфора в чистом виде и серной кислоты. Этот способ заключается в том, что в пластмассовый сосуд наливается серная кислота, затем туда кладется фосфор. Под действием серной кислоты на стенках сосуда образовались через определенное время отверстия, через которые кислота выливалась, а фосфор при соединении с кислородом воздуха воспламенялся. Кроме того, самовоспламенение происходит также при соединении глицерина и марганцовокислого калия, скипидара и азотной кислоты, скипидара и хлора, метилового спирта и перекиси натрия, метилового спирта и хромового ангидрида, ацетона и перекиси натрия, уксусной кислоты и хромового ангидрида. Иногда, злоумышленники, зная условия самовозгорания тех или иных материалов, с целью поджога специально создают ненадлежащим складированием и хранением условия для их самовозгорания. К веществам, способным к самовозгоранию при ненадлежащих условиях хранения, относятся: ископаемый уголь, торф, древесный уголь, негашеная известь, шерсть, хлопок, лен, конопля и др. Для поджогов часто используются приспособления с часовыми механизмами. Такие приспособления дают возможность поджигателю наметить и совершить поджог, находясь далеко от поджигаемого объекта.

Методы и средства взлома компьютерных сетей общего и специального назначения. Программное обеспечение любой компьютерной сети состоит из трех основных компонентов: операционной системы (ОС), сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все методы и средства взлома компьютерных сетей можно разделить на три группы: атаки на уровне ОС; на уровне СПО и на уровне СУБД [21, 23, 25].

Атаки на уровне СУБД являются одной из наиболее трудных задач. Это связано с тем, что все современные СУБД имеют строго определенную внутреннюю структуру, и операции над их элементами заданы довольно четко. В большинстве случаев злоумышленники предпочитают взламывать защиту компьютерной системы на уровне ОС и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или, содержащая ошибки, или, если при определении политики безопасности администратором были допущены ошибки, то становится вполне вероятным преодоление защиты, реализуемой на уровне СУБД. Кроме того, имеются два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы. В первом случае результаты арифметических операций над полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи. Во втором случае злоумышленник получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея атаки на СУБД – так сформулировать запрос, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

Атаковывать операционную систему, в отличие от СУБД, проще. Злоумышленникам, как правило, известны типы используемых ОС, и они располагают методами и средствами их взлома:

– кражу пароля или получение пароля из файла, в котором он был сохранен пользователем;

– кражу внешнего носителя парольной информации (дискеты, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);

– полный перебор всех возможных вариантов пароля или подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе – его имени, фамилии, номера телефона, даты рождения и т. д.;

– сканирование жестких дисков компьютера (злоумышленник последовательно

пытается обратиться к каждому файлу, хранимому на жестких дисках; если объем дискового пространства достаточно велик, можно быть вполне уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны злоумышленником, который для сокрытия следов может организовать эту атаку под чужим именем: например, под именем пользователя);

– сборка «мусора» (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, злоумышленник может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным пользователями: например, просмотрев содержимое их «мусорных» корзин);

– превышение полномочий (используя ошибки в программном обеспечении или в администрировании, злоумышленник получает полномочия, превышающие полномочия, предоставленные ему действующей политикой безопасности);

– подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;

– захват ресурсов (программа производит захват ресурсов, а затем входит в бесконечный цикл);

– бомбардировка запросами (программа постоянно направляет операционной системе запросы, реакция на которые требует значительных ресурсов компьютера).

Атаки на уровне СПО наиболее эффективны, поскольку каналы связи, по которым передаются сообщения, чаше всего не защищены или защищены не достаточно. На этом уровне возможны следующие способы нарушения безопасности:

– прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер злоумышленника подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);

– перехват сообщений на маршрутизаторе (если злоумышленник имеет доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);

– создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида злоумышленник добивается, чтобы его компьютер стал маршрутизатором сети, после чего он получает доступ ко всем сообщениям);

– навязывание сообщений (отправляя сообщения с ложным обратным адресом, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и получает права пользователей);

– отказ в обслуживании (злоумышленник отправляет в сеть сообщения специальною вида, после чего одна или несколько компьютерных систем, подключенных к сети, выходят из строя).

Средства подавления помехами систем ГЛОНАСС (GPS)и мобильной связи. первоначально разрабатывались для военных целей, но с развитием технологий стали доступны и для злоумышленников. К их числу можно отнести. *Сова GPS mini* – одно из самых эффективных устройств в своём ценовом сегменте. Средство российского производства, подавляет частоты стандарта GPS, GSM, ГЛОНАСС. Диапазон частот 1500-1600 МГц. Мощность: 0,6 Вт. *Беркут 12* (сотовая связь и навигация – 20 частот) – создаёт шум, мешающий навигационному позиционированию, работе сотовой связи, устройствам для прослушивания, работе систем скрытого видеонаблюдения и срабатыванию взрывных устройств. *CARCAM SIGNAL JAMMER PS-80N* – походный подавитель радиосигналов с радиусом действия 20 метров. Прибор подавляет радиосигналы в диапазонах: *GSM, 3G, 4G LTE, GPS, 4G WMAX, Wi-Fi.* Эти и им подобные средства могут использоваться злоумышленниками для нарушения контроля перевозки ценных грузов.

Химически опасные и ошеломляющие вещества – химические соединения, обладающие определенными токсическими и физико-химическими свойствами, обеспечивающими при их применении поражение людей, заражение воздуха, местности, техники и строений. Среди таких веществ газы и аэрозоли – самые распространенные. В криминальной практике находят приме-

нение общетоксические (оксид углерода, сероводород, хлорциан), слезоточивые (бромбензилцианид), усыпляющие (фентанил, хлороформ) газы, а также газы, вызывающие панику и дезорганизующие поведение охраны (углекислый газ). Не исключено применение ранцевых распылителей высокого давления типа АРП-16 «Облако», газовых гранат типа «Черемуха», «Сирень», а также средств ошеломляющего (ударного, светозвукового и комбинированного) действия. Типичным примером этих средств являются светозвуковые гранаты – специальное средства не смертельного действия, состоящее на вооружении армии, правоохранительных органов и спецслужб, предназначенное для оказания светозвукового воздействия на противника или правонарушителя с целью временного психофизиологического (отвлекающего и ошеломляющего) и механического иммобилизующего действия для временного вывода его из строя. Как правило, светозвуковые гранаты применяются правоохранительными органами в ходе задержания особо опасных преступников, освобождения заложников, пресечения групповых хулиганских проявлений или массовых беспорядков, а так же войсковым спецназом для захвата противника живым.

Основными факторами воздействия являются громкий звук взрыва и яркая вспышка, которые приводят к временной слепоте и глухоте лиц, находящихся в непосредственной близости от эпицентра взрыва, что на некоторое время лишает их возможности оказывать эффективное сопротивление. Корпус гранаты обычно изготовлен либо из хрупкого пластика, разрушающегося на мелкие осколки, не причиняющие особого вреда, либо из металлического контейнера, не разрушающегося при взрыве совсем, с отверстиями для выхода взрывных газов. Некоторые гранаты дополнительно снаряжены резиновой картечью для оказания травматического действия на правонарушителя. Такие гранаты во время взрыва, помимо яркой вспышки и громкого звука, разбрасывают в стороны резиновую картечь, причиняя травмы (ушибы мягких тканей, подкожные гематомы).

Дистанционно-пилотируемые летательные аппараты (ДПЛА) стали применяться злоумышленниками для доставки на территорию охраняемых объектов взрывчатых устройств, оружия и других предметов. Типичным примером ДПЛА может служить квадрокоптер *DJI Mavic 2 Enterprise Advanced*, находящийся в свободной продаже. Защита от нежелательного проникновения на режимную территорию ДПЛА состоит в том, чтобы либо подавить помехами канал управления аппаратом, либо перехватить управление и посадить его в обозначенном месте. В последнем случае при подлете аппарата к охраняемой территории происходит срабатывание системы обнаружения, она определяет его уникальный идентификационный номер, после чего приступает к захвату управления им. Естественно, что проведение такой операции требует привлечения соответствующих технических средств.

Средства дистанционного подрыва взрывных устройств находят все большее применение у террористов, как в нашей стране, так и за рубежом [13,14]. Этому способствуют следующие основные причины:1) возможность заблаговременной установки радиоуправляемого взрывного устройства на месте совершения террористического акта; 2) управление подрывом осуществляется на безопасном расстоянии (50 метров и более), тем самым, обеспечивается скрытность действий организатора взрыва, а так же приведение его в действие в любой выбранный момент времени. Радиоуправляемое взрывное устройство может быть размещено в любом трудно поддающемся обнаружению камуфляже или скрытно размещено на поверхности земли, в грунте, в строениях, в запаркованном автомобиле, уличной урне и в многочисленных других местах и предметах, что делает практически невозможным выявление взрывного устройства методом визуального контроля. Наиболее часто в террористических целях применяются непрофессионально или кустарно изготовленные радиовзрывные устройства. Основная опасность непрофессионально изготовленных РВУ заключается в непредсказуемости их реакции на внешнее воздействие. Постановка радиопомех непрофессиональным радиолиниям вместо ожидаемого эффекта подавления канала управления может привести к взрыву боеприпаса. Часто преступники для снижения риска самоподрыва на таких устройствах используют разнообразные таймеры, которые дают задержку по включению боевой части, тем самым, оберегая свою жизнь и подвергая опасности жизни окружающих. В носимом варианте исполнения выходная мощность передатчика мо-

жет составлять от долей до единиц Ватта. При использовании автомобильной радиостанции, выходная мощность передатчика может достигать нескольких десятков Ватт. В этом случае дальность подрыва может быть значительно больше, чем для носимого передатчика и достигать нескольких километров, но как правило чаще всего наиболее вероятное значение дальности действия составляет от 50 до 400 м, при мощности управляющего передатчика до 0,1 Ватта. Максимально допустимое время от момента включения (установки) прибора до подачи команды на подрыв определяется емкость источников питания, которые постепенно истощаются, расходуя заряд на поддержание работы радиоприемника. Так как в большинстве случаев используются малогабаритные источники питания, то их емкость невелика. Однако небольшая емкость может компенсироваться дежурным режимом работы приемно-исполнительного прибора, при котором отключены все сильноточные цепи, кроме тех, которые обеспечивают прием сигнала кодированной команды. Соответственно, если удастся заблокировать ожидаемый приемным устройством кодированный сигнал управления РВУ, то удастся предотвратить его срабатывание. Это может быть достигнуто постановкой помех достаточной мощности, чтобы гарантированно перекрыть управляющий сигнал. При этом нет необходимости постановщику радиопомехи достигать мощности большей, чем мощность управляющего устройства, поскольку постановщик помех как правило находится к РВУ значительно ближе, чем управляющий передатчик.

Заключение. В целом следует заключить, что злоумышленники и преступные элементы, в ходе развития и совершенствования своих средств и приемом, могут более полно реализовать и расширить схему преодоления барьеров безопасности КВОСИ. При этом следует ожидать, что чем развитее и эффективнее становится система управления обеспечением безопасности этих объектов, тем больше усилий будут направлять преступные элементы на ее нейтрализацию и дезорганизацию процессов ее функционирования. Перечисленными обстоятельствами диктуется настоятельная необходимость постоянной модернизации средств и систем обеспечения безопасности КВОСИ, а также совершенствования управления ими с целью гарантированного опережения злоумышленников и преступных элементов.

ЛИТЕРАТУРА

1. Федеральный закон РФ от 26.07.2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ, 31.07.2017, N 31 (Ч I), ст. 4736.

2. Федеральный закон от 21.12.1994 N 69-ФЗ (ред. от 23.06.2016) «О пожарной безопасности».

3. Приказ Минюста России от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы».

4. Доронин А. И. Бизнес-разведка / А. И. Доронин. – М.: Ось-89; Издание 3-е, пер. и доп., 2014. – 281 с.

5. Джилад Б. Конкурентная разведка. Как распознать внешние риски и управлять ситуацией. – СПб.: Питер, 2010. – 320 с.

6. Нежданов И. Ю. Технологии разведки для бизнеса / И. Ю. Нежданов. – М.: Ось-89, 2009. – 400 с.

7. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова – Ст. Оскол: ТНТ, 2010. – 384 с.

8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В. В. Гафнер. – Рн/Д: Феникс, 2017. – 324 с.

9. Измалков А.В. Управление безопасностью социально-экономических систем и оценка его эффективности / А. В. Измалков. – М.: Спутник+, 2003. – 441 с.

10. Фомин А. В. Анализ методов управления пожарной безопасностью объектов защиты / А. В. Фомин, В. П. Мочалов, // Научно-аналитический журнал «Вестник Санкт-Петербургского университета МЧС России». – 2011. – С. 19-23.

11. Калыгин В. Н. Безопасность жизнедеятельности. Промышленная и экологическая безопасность в техногенных чрезвычайных ситуациях. Учебное пособие для ВУЗов / В. Н. Калыгин. – М.: Колос, 2013. – 586 с.

12. Багера И. Н. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи / И. Н. Багера // Из-

вестия Юго-Западного государственного университета. – 2016. – № 4. – С. 88-95.

13. Рудаков Б. В. Проблемы эффективного применения средств нейтрализации взрывных устройств в правоохранительной деятельности / Б. В Рудаков, Д. Ю. Кияницына // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 171–175.

14. Можаев С. Н. Взрывные устройства, используемые террористами при совершении террористических актов / С. Н. Можаев. – М.: ЦОКР МВД России, 2010. – С. 76-98.

TECHNICAL MEANS OF INTENTIONALLY VIOLATING THE SECURITY OF CRITICAL SOCIAL INFRASTRUCTURE FACILITIES

© 2021 D. E. Orlova

Voronezh Institute of the Federal Penitentiary Service of Russia (Voronezh, Russia)

A brief overview of modern technical means that can be used by intruders and criminal elements to intentionally violate the security of critical social infrastructure objects is given. These data can be used in the bodies that ensure the safety of these facilities, as well as in the modeling and optimization of integrated security processes.

Keywords: security, critical object, technical means.